

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
18 October 2001 (18.10.2001)

PCT

(10) International Publication Number
WO 01/78024 A2(51) International Patent Classification⁷: G07F 19/00,
G06F 17/60

(21) International Application Number: PCT/US01/11911

(22) International Filing Date: 11 April 2001 (11.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/195,963 11 April 2000 (11.04.2000) US
09/809,367 15 March 2001 (15.03.2001) US(71) Applicant: MASTERCARD INTERNATIONAL
INCORPORATED [US/US]; 2000 Purchase Street,
Purchase, NY 10577-2509 (US).(72) Inventors: HOGAN, Edward, J.; 14 N. Chatworth Ave-
nue, Larchmont, NY 10538 (US). CAMPBELL, Carl,
M.; 809 Marlin Road, Newton Square, PA 19073 (US).(74) Agent: SCHEINFELD, Robert, C.; Baker Botts L.L.P.,
30 Rockefeller Plaza, New York, NY 10112-0228 (US).(81) Designated States (*national*): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,
CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM,
HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,
LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX,
MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL,
TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.(84) Designated States (*regional*): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian
patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European
patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,
IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF,
CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished
upon receipt of that reportFor two-letter codes and other abbreviations, refer to the "Guid-
ance Notes on Codes and Abbreviations" appearing at the begin-
ning of each regular issue of the PCT Gazette.(54) Title: AN IMPROVED METHOD AND SYSTEM FOR CONDUCTING SECURE PAYMENTS OVER A COMPUTER NET-
WORK

(57) Abstract: A method is provided for conducting a financial transaction by a purchaser with a merchant having an acquirer bank, over a communications network. The method includes the steps of sending a first authorization request using a pseudo account number associated with a real account number to a service provider which forwards a second authorization request to the issuer using the real account number and preferably a pseudo acquirer code associated with the service provider such that the response to the second request is based on the real account number and sent back to the service provider who preferably forwards a response to the first request preferably to the "real" acquirer. A message authentication code is further provided which includes transaction data, and where the authorization request is formatted as a standard payment card track having one or more fields including a discretionary field in which the message authentication code is placed.

WO 01/78024 A2

**AN IMPROVED METHOD AND SYSTEM FOR CONDUCTING
SECURE PAYMENTS OVER A COMPUTER NETWORK**

SPECIFICATION

PRIORITY APPLICATIONS

5 This application claims priority to United States provisional
application 60/195,963, filed on April 11, 2000, and entitled "Method and System for
Conducting Secure Payments Over A Computer Network," which is hereby
incorporated by reference, and to United States application serial number 09/809,367,
filed March 15, 2001, and entitled "Method and System for Secure Payments Over A
10 Computer Network," also incorporated by reference.

BACKGROUND OF INVENTION

 This invention relates to a method and system for conducting secure
financial transactions over a communications network and more particularly to a
method and system for transmitting payments securely over a computer network, such
15 as the Internet, and for transmitting sensitive information securely over public
communication channels.

 As is self-evident, on-line commerce has experienced tremendous
growth over the last few years but even with that growth consumers are still troubled
and concerned about using personal financial information and transmitting such
20 information, such as credit card numbers and personal identification numbers, over
public communications networks, such as the Internet. As a result, over the last few
years, companies have struggled to find a way -- the best way -- to ensure the security
of payments made over a computer network and to decrease the risk of theft or misuse
of financial information.

25 For example, U.S. Patent No. 5,883,810 entitled "Electronic Online
Commerce Card With Transaction Proxy Number For Online Transactions" and
assigned to Microsoft Corporation, is directed to a system which provides for each
transaction a temporary transaction number and associates it with the permanent
account number; the transaction number looks like a real credit card number and the
30 customer uses that transaction number and submits it to the merchant as a proxy for

the customer account number. In this matter, the customer does not have to transmit over a public network his or her real credit card number.

5 In the '810 patent, the merchant passes along the transaction number to the issuing institution, which in turn uses the transaction number as an index, accesses the real customer account number and processes the authorization, sending the authorization reply back to the merchant under the transaction number. As a result, risk is purportedly minimized not only because the customer only transmits a transaction number but also because the proxy number is good only for a single purchase -- theft "would not greatly benefit a thief because it cannot be repeatedly
10 used for other purchases or transactions." Col. 2, lines 60-61.

There is a need to improve upon the prior art systems and in particular there is a need for a method and system for conducting a secure financial transaction over the Internet which avoids requiring the creation and transmission of a unique repeatedly generated transaction number to replace the transmission of the permanent
15 account number for each conducted transaction.

According to the invention of co-pending application 09/809,367, filed March 15, 2001, which is incorporated herein by reference, a "pseudo" account number is assigned to a customer and cryptographically linked to a consumer's payment account number. The payment account number is an account number issued
20 by a financial institution or other organization that a consumer may use to make a payment for goods and/or services. For example, the payment account number may be the account number from a payment card, such as a credit or debit card, or from a payment application, such as an electronic cash application stored on a consumer's computer. The pseudo account number appears to be an actual payment account
25 number to a merchant. That is, the pseudo account number has the same length as a valid payment account number and begins with a valid identification number (e.g., a "5" for MasterCard International Incorporated ("MasterCard")). The pseudo account number is used by the customer instead of the real account number for all of his or her on-line financial transactions.

30 According to the invention of the co-pending application 09/809,367, all transactions based on pseudo account numbers are preferably cryptographically

authenticated using a secret key that is unique for each account number. The authentication may be based on the private key of a public-key pair ("public-key authentication"), or based on a secret key other than a private key ("secret-key authentication"). Thus, if unauthorized persons were to ascertain any pseudo account numbers, they would be unable to make fraudulent transactions using them.

This system can still be improved upon and security can be further enhanced to protect the messages and information being transmitted during or in connection with a financial transaction being conducted over public communications lines.

10

SUMMARY OF INVENTION

According to the present invention, therefore, a method of conducting a transaction using a payment network is provided, in which a service provider receives a first authorization request for the authorization of a transaction using a first payment account number, wherein:

15

(i) the first payment account number has a BIN code associated with the service provider, and is associated with a second payment account number having a BIN code associated with an issuer of said second number;

20

(ii) the first authorization request includes an acquirer code associated with an acquirer; and
(iii) the first authorization request is routable through the payment network to the service provider based on the BIN code of the first payment account number.

25

The method further includes having the service provider respond to the first authorization request by transmitting a second authorization request for authorization of the transaction using the second payment account number, the second authorization request including an acquirer code associated with the service provider and being routable through the payment network to the issuer based on the BIN code of the second payment account number.

30

Additionally, a response to the second authorization request is received by the service provider from the issuer, where the response includes the acquirer code associated with the service provider and is routable through the payment network based on that code. A response to the first authorization request is then transmitted by the service provider to the acquirer based on the response to the second authorization request, and the response to the first authorization request preferably includes the acquirer code associated with the acquirer and is routable through the payment network based on that code.

Another preferred embodiment of the invention includes a method of conducting a transaction with a merchant using a first payment account number that is associated with a second payment account number, where the method comprises: (a) generating a message authentication code based on one or more transaction details; (b) transmitting at least the first payment account number and the message authentication code to the merchant; (c) requesting by the merchant an authorization for payment of the transaction using the first payment account number, the request being formatted as if payment were tendered at a point-of-sale terminal with a conventional magnetic-stripe payment card, the message authentication code being transmitted in a discretionary data field contained in a track of the type used in the magnetic stripe of said conventional payment card; (d) responding to the authorization request for the first payment account number by requesting an authorization for payment of the transaction using the associated second payment account number; and (e) accepting or declining the authorization request for the first payment account number based on the response to the authorization request for the second payment account number and the message authentication code.

BRIEF DESCRIPTION OF THE DRAWINGS

Further objects, features and advantages of the invention will become apparent from the following detailed description taken in conjunction with the accompanying figures showing a preferred embodiment of the invention, on which:

FIG. 1 is a block diagram of the system for obtaining a secure payment application from a provider over the Internet in accordance with the invention;

FIG. 2 is a flow diagram illustrating the flow of information between a cardholder and a merchant when conducting a secure payment over the Internet using the present invention;

FIG. 3 is a flow diagram illustrating the flow of information between an acquirer, a service provider and an issuer, in accordance with the present invention;

FIG. 4 is a flow diagram illustrating the flow of information between an issuer, a service provider and an acquirer, in accordance with the present invention;

FIG. 5 is a flow diagram illustrating the flow of communication between a merchant and an acquirer for purposes of settlement and clearing, in accordance with the present invention;

Throughout the figures, the same reference numerals and characters, unless otherwise stated, are used to denote like features, elements, components or portions of the illustrated embodiment. Moreover, while the subject invention will now be described in detail with reference to the figures, it is done so in connection with a preferred embodiment. It is intended that changes and modifications can be made to the described embodiment without departing from the true scope and spirit of the subject invention as defined by the appended claims.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Initialization of the Secure Payment Application

In accordance with a preferred embodiment of the invention, a service provider issues, maintains and/or processes several components, including a secure payment application ("SPA"), of the secure payment system to be conducted in accordance with the techniques of the present invention.

Figure 1 illustrates first how a cardholder with a financial transaction card may obtain a secure payment application from the service provider over the Internet, according to an exemplary embodiment of the present invention. It should initially be understood that a physical card is not necessary to utilize and obtain the benefits of the invention, but that only an account number be issued to a holder (in this case a cardholder) which identifies and links a user or participant to an account for purposes of conducting a financial transaction. The cardholder may contact a web server associated with the service provider using any appropriate device that may

communicate over the Internet, such as a computer, cellular phone, or a personal digital assistant (PDA). For the purpose of simplicity in the following discussions, it is assumed that the cardholder uses a computer to communicate over the Internet.

As shown in Fig. 1, the service provider, for example MasterCard International Incorporated (or an agent of MasterCard), has in its control one or more physically secure security modules 12, which offer physical protection for the information stored inside the modules. These security modules each contain one or more "derivation keys" that are used to create and re-create account-unique secret cryptographic keys, as explained below, which are provided within the secure payment application.

First, in accordance with a preferred embodiment of the invention, the cardholder must obtain an SPA from the service provider. The preferable steps for downloading and initializing the secure payment application (SPA) include:

1. The cardholder contacts the service provider's web site via the Internet (either directly or through a hyperlink to the web site through another web site, such as an issuer's web site.
2. The cardholder provides, under SSL encryption generally known to those skilled in the art, (a) a payment card account number, (b) a card expiration date, and (c) card authenticating information. The card authenticating information may include, for example, the card's CVC2 value, which refers to a three or four digit value that is printed next to the signature panel of some cards. This value is generated by the issuing bank using a secret cryptographic key and can be verified using this same key.
3. The service provider may confirm the legitimacy of the card account number and the card expiration date by obtaining a zero amount authorization from the issuer of the cardholder's payment card. For instance, MasterCard may obtain this authorization over its Banknet™ communications network.
4. The service provider may verify the CVC2 value if the issuer of the cardholder's payment card has provided the service provider with the cryptographic key(s) for verifying the CVC2 value.

5. The service provider may verify other card authenticating information by sending such information to the issuer for verification.
6. After the service provider ("SP") has confirmed the legitimacy of the cardholder-provided card data, the SP creates or selects a pseudo account number and a secret key and embeds these data elements into a secure payment software application that is made available to the cardholder for download over the Internet preferably under SSL encryption.

The pseudo account number has as its BIN a special BIN reserved for pseudo account numbers. The remainder of the pseudo account number is a value that can be translated by the service provider via a table look-up process to the "real" account number.

Preferably, the assigned special service provider BIN may be one from a set of many such special BINs, where each BIN may correspond to a particular country or region and/or to a particular product within a country or region. Thus, the assigned special BIN may be the one that corresponds to the country and/or the product of the submitted "real" account number.

The secret key that the service provides preferably embeds in an SPA is unique for each card account number and is preferably derived within a security module using the card account number and a derivation key. This derivation key may itself be derived within the same or another security module using a higher-level derivation key.

The cardholder may provide a password to the service provider prior to downloading the secure payment application or may select a password when the secure payment application is being installed on the cardholder's computer. If a password is provided or selected, the cardholder will thereafter be required to enter this password in order to activate the secure payment application. The password selected by the cardholder may be used to encrypt the secret key included in the SPA.

As would be recognized by those skilled in the art, the SPA may be downloaded as part of a digital wallet application. In addition to the SPA, the digital wallet may store a cardholder's personal information and other applications, such as a purse application.

Generating Card-Unique Secret Keys

The following steps may preferably be performed within a security module 12 controlled by the service provider or one of its agents to obtain a card-unique secret key to be included in the secure payment application. The following steps assume that the cardholder's payment card has a 16-digit account number and that the Data Encryption Algorithm (DEA) known to those skilled in the art, with a double-length key is used. The DEA is a U.S. Government standard cryptographic algorithm that is described in Federal Information Processing Standard (FIPS) 46-1, which is incorporated herein by reference in its entirety. The DEA is also defined in the ANSI standard X9.32, which is also incorporated herein by reference in its entirety.

It is also assumed that the security module holds a secret high-level key called the derivation key that consists of 16 bytes and is used with many or all card account numbers to cryptographically compute a card-unique secret key, called the Per-Card Key, given the cardholder's 16-digit payment account number. The derivation key may be unique for each country or for each special bank identification number or BIN.

Preferably, the steps are:

1. Considering the payment account number as 16 binary-coded-decimal digits of 4 bits each, DEA-encrypt these 64 bits using as the encryption key the left-most 8 bytes of the 16-byte Derivation Key.
2. DEA-decrypt the result of Step 1 using as the decryption key the right-most 8 bytes of the 16-byte Derivation Key.
3. DEA-encrypt the result of Step 2 using as the encryption key (again) the left-most 8 bytes of the 16-byte Derivation Key.
4. Use the result of Step 3 as the left-most 8 bytes of the unique Per-Card Key.
5. DEA-encrypt the result of Step 3 using as the encryption key the left-most 8 bytes of the 16-byte Derivation Key.
6. DEA-decrypt the result of Step 5 using as the decryption key the right-most 8 bytes of the 16-byte Derivation Key.

7. DEA-encrypt the result of Step 6 using as the encryption key (again) the left-most 8 bytes of the 16-byte Derivation Key.
8. Use the result of Step 7 as the right-most 8 bytes of the 16-byte unique Per-Card Key, and place this key in the secure payment application in such a way
5 that it will not be disclosed during the normal operation of this application.

Communication Between Cardholder and Merchant

Fig. 2 illustrates the flow of information between the cardholder 14 and merchant 16 when conducting a secure payment over the Internet according to an exemplary embodiment of the present invention.

10 Once the SPA has been installed on a cardholder's computer, the cardholder preferably uses the SPA for all Internet payments and the SPA provides the cardholder's pseudo account number for all Internet transactions.

Once a cardholder has indicated a desire to conduct a transaction, it is desirable (but not essential) that the merchant pass to the cardholder's computer the
15 following data elements: (1) the acquirer BIN, (2) the MID (the merchant identifier as known to the acquirer), and (3) the date and time (GMT or equivalent) of the transaction.

Preferably, the SPA uses its embedded, secret key to create a Message Authentication Code (MAC) relating to the transaction. For example, a MAC of
20 approximately 8 decimal digits may be created on the following data elements:

1. A transaction sequence number stored in the cardholder's SPA and incremented by the SPA whenever it generates a MAC. This transaction sequence number may be, for example, six (6) decimal-digits in length.
2. The acquirer BIN if received from the merchant, otherwise zeros (which may
25 be, for example, 6 decimal digits).
3. The MID if received from the merchant, otherwise zeros (which may be, for example, 6 decimal digits).
4. Date and time, to the nearest hour or minute (in GMT), if received from the merchant, otherwise zeros (which may be, for example, 10 decimal digits).

5. The transaction amount, as displayed for the cardholder, and as normally included in the message from cardholder to merchant (which may be, for example, 8 decimal digits).

5 Preferably, a merchant is able to accept a full Track-1 image from the cardholder's computer, just as if the merchant were prepared to communicate with computers that include magnetic-stripe readers. (The Track-1 image refers to the data on track 1 of the magnetic stripe of a payment card.) Moreover, the merchant preferably is able to pass the Track-1 data to the acquirer as if the transaction were a point-of-sale (POS) transaction.

10 If the merchant can accept the full Track-1 data, the MAC itself and the data elements upon which the MAC is based are placed in the Track-1 discretionary-data field. The pseudo account number is placed in the Track-1 account-number field, and the card expiration date is placed in the Track-1 expiration-date field.

15 By sending the MAC in the Track-1 discretionary-data field, many merchants will not need to make any changes to their systems and/or software because they can already handle POS transactions, which include Track-1 discretionary data. For other merchants, systems and/or software to handle POS transactions are readily available.

20 If a merchant cannot accept the full Track-1 data, the SPA may send a conventional SSL payment message, except that the pseudo account number is used instead of the cardholder's "real" account number. The merchant then sends the transaction data to the acquirer in the manner that it normally does. In practice, during a transition period, the merchants that are not capable of handling POS transactions with Track-1 data might not be required to receive and handle MACs.

25 Instead of being sent in the Track-1 discretionary-data field, the MAC may also be sent in another format, in which case merchants and acquirers may be required to change their systems and/or software to handle this other format.

30 Upon receipt of the cardholder's transaction message, the merchant formats a conventional authorization request for the acquirer. For those merchants that are able to accept Track-1 data, this authorization request will be

formatted exactly as if it originated from a POS terminal and will include the Track-1 data provided by the cardholder.

Should a merchant initiate multiple authorization/clearing transactions for a cardholder transaction, preferably only the first of these transactions will include the Track-1 data. The subsequent transactions will include only the pseudo account number and expiration date and may be considered mail-order-telephone-order transactions. This is true for all recurring payments and partial payments with multiple clearings.

Acquirer Handling of Authorization Request

Fig. 3 illustrates the communication between an acquirer 18, service provider 10, and an issuer according to an exemplary embodiment of the present invention.

The presence of Track-1 data in an Internet transaction should not adversely impact those acquirers who receive transactions from Internet merchants via conventional telephone lines, since such transactions will be formatted identically to transactions from conventional point-of-sale terminals. However, acquirers who receive transactions via the Internet (and not conventional telephone) may need a "conversion box" that would deliver transactions without Track-1 data unchanged and would deliver transactions with Track-1 data over a different physical wire as if they had come from POS terminals. The design of such a conversion box is well within the ability of a person of ordinary skill in the art.

When an acquirer 18 receives an authorization request message from an Internet merchant 16, it looks up the issuer BIN in its BIN table. In the case of a pseudo account number transaction, the "issuer" will correspond to a service provider-authorized processing facility 10, which will receive the request. In the case of a non-pseudo or real account number, normal processing will take place.

Some countries may have a special security-module-equipped facility that handles domestic transactions. Each such domestic facility would preferably be set up only with the service provider's approval and would hold only the cryptographic keys and account-number conversion data for the country whose transactions it processes. In countries with such a domestic facility, all same-country

transactions will be sent to this facility. This can also be done for individual banks in a country, if it is so desired.

A domestic facility to handle domestic transactions would be far more efficient than causing domestic transactions to go through a central processing

5 facility.

Service Provider Handling of the Authorization Request

When the service provider receives the request, it determines from the issuer BIN whether the account number is really a pseudo account number and, if so, sends the transaction to a special system for processing. This system translates the
10 pseudo account number to the "real" account number using a table-lookup procedure. If the system determines that a Track-1 image is included, it uses a security module to derive the appropriate Per Card Key for this card account number in order to verify the MAC. (The derivation of the Per Card Key is described above.)

If the MAC is verified, the system then examines the BIN in the Track-
15 1 discretionary-data area. If this is not all zeros, the system compares this BIN with the acquirer BIN of the transaction, and verifies that the date and time included in the Track-1 discretionary-data area are reasonable (taking into consideration that the merchant may batch its transactions and obtain delayed authorizations). The system also verifies that the authorization request amount does not exceed the transaction
20 amount in the Track-1 discretionary-data area (the amount as approved by the cardholder) by more than a specified amount (e.g., 20%).

It is possible that an acquirer may include the MID in the Acquirer Reference Data (which is also called the Acquirer Reference Number). It is assumed that the 23-digit Acquirer Reference Data includes a mandatory "transaction type"
25 indicator and a mandatory acquirer BIN, but that the remaining digits are for the acquirer's discretionary use and may in some cases include the MID. The service provider may obtain from its Internet acquirers an indication of which acquirers include the MID in the Acquirer Reference Data, and if so, where in the Acquirer Reference Data they include it. In the case of such an acquirer, if the Track-1 image
30 includes an acquirer BIN (rather than six zeros), the service provider system may also

verify that the MID in the Track-1 discretionary-data area matches the MID in the Acquirer Reference Data.

The service provider system may store a history of transaction sequence numbers (TSNs) for comparison with transaction sequence numbers in authorization requests. The comparison may be triggered by some condition, such as when the Track-1 amount exceeds some specified threshold (e.g., \$200). Such a threshold may be lower when the Track-1 image does not include an acquirer BIN. When the comparison is triggered, the system may compare the transaction sequence number included in the Track-1 discretionary-data area against the stored history of transaction sequence numbers for the relevant card account number. If the transaction sequence number of the current transaction is 1) higher than the smallest stored value for the current account number and 2) does not match any stored value for this account, there is a reasonable assurance that the current transaction is not the fraudulent replay of data from a previous legitimate transaction.

The stored history of TSNs may be limited to a predetermined number of TSNs. For example, the system might store only the last 10 transaction sequence numbers received for a particular card account number. In addition, the verification of transaction sequence numbers need not occur in real time. It may occur while the system is obtaining an authorization from an issuer.

The purpose of these checks is to make it very difficult for wrongdoers who operate in collusion with Internet merchants and who may be able to obtain unencrypted transaction data to fraudulently replay data from legitimate transactions.

Once the service provider system has completed the above-described verification processes (with the possible exception of the transaction sequence number verification), the system formats an authorization request message for the issuer. This message includes the "real" account number and expiration date, but excludes the other Track-1 data. The system replaces the acquirer BIN with one of the special BINs that serves as a "pseudo" acquirer BIN. The acquirer BIN is replaced so that the issuer responds to the service provider instead of the acquirer.

In order for the acquirer and issuer to compute interchange fees correctly, the pseudo acquirer BIN should preferably correspond to the country in

which the acquirer is located or to another country or region that will provide the same resultant interchange fees. If each country has a special BIN associated with it, the service provider may replace the acquirer BIN with the special BIN associated with the acquirer's country. If an acquirer's country does not have a special BIN
5 associated with it, a special BIN associated with another country may be selected that results in the same interchange fees.

The service provider stores in a database the Acquirer Reference Data received in the authorization request from the acquirer (hereinafter referred to as the "original Acquirer Reference Data"). In formatting an authorization message for the
10 issuer, the service provider preferably replaces the original Acquirer Reference Data with "pseudo" Acquirer Reference Data that includes the pseudo acquirer BIN, an appropriate transaction-type indicator, and an index value that the service provider can use to find the original Acquirer Reference Data.

When a domestic facility processes a pseudo-account-number
15 transaction, it operates as described above. Preferably, however, this domestic facility will process only transactions for domestic issuers, and therefore will need only the cryptographic keys and account-number conversion table entries that apply to that country.

Issuer Handling Of Authorization Request

20 Fig. 4 illustrates the communication between the issuer 20, the service provider 10, and an acquirer 18 according to an exemplary embodiment of the present invention after the issuer has received an authorization request from the service provider or from an authorized domestic processing facility.

The issuer 20 authorizes the transaction just as it would any other
25 transaction. It sends the authorization response back to the "pseudo" acquirer BIN, which will be either a service provider facility or a facility authorized by a service provider.

When the service provider 10 receives an authorization response from an issuer, it examines the acquirer BIN to determine whether it is a "pseudo" acquirer
30 BIN. If so, the service provider determines that the authorization response corresponds to a pseudo account number transaction that must be "restored" to its

original format. Thus, the service provider translates the “real” account number back to the pseudo account number, and restores the Acquirer Reference Data that had been in the original transaction. The service provider then transmits the resulting message to the “real” acquirer, which processes the transaction normally and sends the authorization response to the merchant in the normal way. The merchant responds to the authorization response as it would for any other transaction.

Settlement and Clearing

Figure 5 illustrates the flow of communication between a merchant 16, an acquirer, service provider or payment processor, for example, MasterCard’s Banknet, and an issuer for the purpose of settlement and clearing according to an exemplary embodiment of the present invention.

A clearing message is processed essentially in the same manner as an authorization request message. As previously described, the acquirer 18 (because of entries in its BIN table) automatically routes a clearing message using a pseudo account number preferably to the service provider 10 or payment processor. At this facility, the pseudo account number is replaced by the “real” account number, the acquirer BIN is replaced by the “pseudo” acquirer BIN, and the remainder of the Acquirer Reference Data is replaced by an index that the service provider can subsequently use to obtain the original Acquirer Reference Data. The clearing message with these changes is transmitted to the “real” card issuer 20, which processes the transaction in the normal way. If the acquirer happens to also be the issuer, the service provider returns the cleared transaction to the acquirer with the real account number and proper fee calculations.

Exception Processing

When a message about a transaction must be transmitted back to the acquirer or merchant from an issuer, the message is processed by the issuer as it normally would process any transaction message. Since the transaction as known to the issuer includes the “pseudo” acquirer BIN, the “pseudo” acquirer BIN will cause the transaction message to be routed to a service provider facility. At this facility the “real” account number is replaced by the pseudo account number, and the pseudo

Acquirer Reference Data is replaced with the original Acquirer Reference Data. The transaction message is then routed to the acquirer, which processes it like any other such transaction message.

Issuance of Plastic Cards for Identification

5 In some situations, a cardholder may buy a ticket over the Internet and will be required, upon showing up at the event to which the ticket grants admission, to produce the card used in the transaction in order to authenticate rightful possession of the ticket.

10 To accommodate such situations, the service provider may issue and mail physical plastic cards to cardholders who obtain pseudo account numbers for Internet use. These cards would clearly indicate "for identification purposes only, not valid for transactions" on them. The embossed and encoded account number would be the pseudo account number, though the CVC2 may be that of the "real" payment card.

15 As another alternative, those merchants that have a legitimate need to authenticate a cardholder using a pseudo account number may register with the service provider (by providing to the service provider appropriate identification and authentication information), and the merchants will be provided with a secret key or certificate as cryptographic proof of their registration. Thereafter, such merchants
20 may obtain "real" account numbers from a service provider facility by providing a copy of the pseudo-account-number transaction details under cryptographic authentication that authenticates both the transaction data and the merchants' right to obtain a "real" account number. The service provider may then forward the "real" account numbers in encrypted form to the merchants, so that the cardholders may be
25 identified with the cards corresponding to their "real" account numbers.

Advantageously, the present invention provides enhanced security for the use of payment account numbers over the Internet.

 The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise numerous
30 systems and methods which, although not explicitly shown or described herein,

embody the principles of the invention and thus within the spirit and scope of the invention.

CLAIMS

1. A method of conducting a transaction using a payment network, comprising:

- 5 (a) receiving by a service provider a first authorization request for the authorization of a transaction using a first payment account number, wherein:
- (i) the first payment account number has a first BIN code associated with the service provider and is associated with a second payment account number having a second BIN code associated with an issuer of
10 said second number, said second payment account number not being included in said first authorization request;
- (ii) the first authorization request includes a first acquirer code associated with an acquirer; and
15 (iii) the first authorization request is routable through the payment network to the service provider based on said first BIN code;
- (b) responsive to the first authorization request, transmitting by the service provider a second authorization request for authorization of the transaction using the
20 second payment account number, the second authorization request including a second acquirer code associated with the service provider and being routable through the payment network to the issuer based on said second BIN code;
- (c) receiving a response to the second authorization request by the service provider from the issuer, the response including the second acquirer code and being
25 routable through the payment network based on that code; and
- (d) transmitting a response to the first authorization request by the service provider to the acquirer based on the response to the second authorization request, the response to the first authorization request including the first acquirer code and being routable through the payment network based on that code.

2. The method of claim 1, wherein said response to the second authorization request from the issuer further includes said second payment account number, and said response to the first authorization request by the service provider further includes said first payment account number.

5 3. The method of claim 1, wherein said first authorization request comprises a message authentication code including transaction data, and said request is formatted with a standard track having a plurality of fields including a discretionary field in which said message authentication code is placed.

4. The method of claim 3, wherein said service provider verifies the
10 message authentication code.

5. A method of conducting a transaction with a merchant over a communications network using a first payment account number that is associated with a second payment account number, the method comprising:

(a) generating a message authentication code based on one or more
15 transaction details;

(b) transmitting at least the first payment account number and the message authentication code to the merchant;

(c) requesting by the merchant an authorization for payment of the transaction using the first payment account number, the request being formatted as if
20 payment were tendered at a point-of-sale terminal with a conventional magnetic-stripe payment card, the format having a track with at least a discretionary data field and said message authentication code being transmitted in said discretionary data field;

(d) responsive to the authorization request for the first payment account number, requesting an authorization for payment of the transaction using the second
25 payment account number; and

(e) accepting or declining the authorization request for the first payment account number based on the response to the authorization request for the second payment account number and the message authentication code.

6. The method of claim 5, wherein said first and second payment account numbers include respective BIN codes, the first associated with a service provider and the second associated with an issuer of the second payment account number, said service provider receiving said merchant's request through a payment network based on said first BIN code, and wherein said service provider generates said request for authorization of payment using the second payment account number and routes said request to said issuer through said network based on said second BIN code.

7. The method of claim 6, wherein said service provider includes in said request for authorization for payment an acquirer code associated with said service provider, such that said response from said issuer is routed back to said service provider.

8. The method of claim 7, wherein said request by said merchant includes an associated merchant acquirer code, and wherein said service provider generates a message based on said accepting or declining step and routes that message to said associated merchant acquirer code.

9. A method of conducting a transaction over a communications network comprising:

issuing by an issuer having an issuer BIN a first payment account number to a user having a computer, said issuer BIN being associated with said first payment account number;

providing a security module for generating a secret key unique to each first account number issued;

generating a second account number associated with said first payment account number;

providing a secure payment application by a service provider to said computer, said application comprising said second account number and said secret key;

storing said secure payment application on said computer;

selecting a merchant with whom to conduct said financial transaction, said merchant having an associated acquirer BIN;
passing to said computer transaction data;
generating a message authentication code based on said transaction data;
5 transmitting track data to said merchant, said track data comprising said message authentication code and said second account number;
generating a first authorization request based on said data;
transmitting said first request to said service provider;
verifying said first request with said secret key;
10 obtaining said first payment account number associated with said second account number;
transmitting a second authorization request using said first payment account number to said issuer BIN associated with said number; and
authorizing or rejecting said second request.

15 10. The method of claim 9, wherein said track data comprises a discretionary data field, an account number field, and an expiration date field, and wherein said transmitting track data step further includes

placing said message authentication data in said discretionary data field;
placing said second account number in said account number field; and
20 placing an expiration date in said expiration date field.

11. The method of claim 10, wherein said transaction data include said associated acquirer BIN, and a transaction amount.

12. The method of claim 11, wherein said verifying step further includes verifying said transaction data.

25 13. The method of claim 9, wherein said second authorization request includes an acquirer code associated with said service provider, and further comprising the steps of:

- generating a message based on said authorizing or rejecting step;
forwarding said message to said service provider based on said acquirer
code; and
using said merchant's associated acquirer BIN to advise said merchant of
5 said message.

1/2

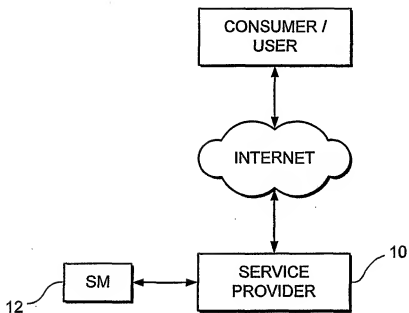


FIG. 1



FIG. 2

2/2

FIG. 3

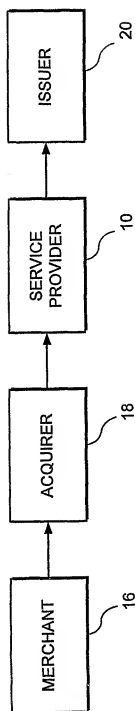


FIG. 4

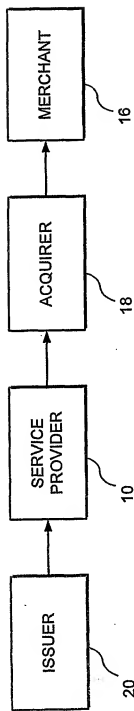
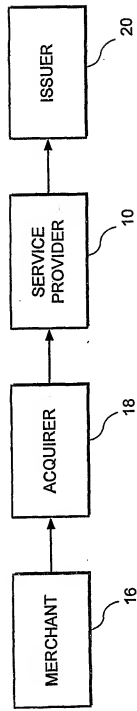


FIG. 5



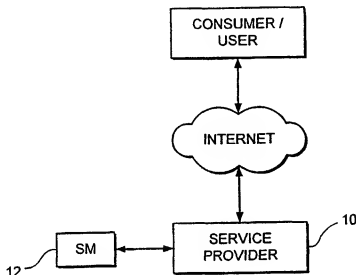
(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
18 October 2001 (18.10.2001)

PCT

(10) International Publication Number
WO 01/78024 A3

- (51) International Patent Classification: G07F 19/00, G06F 17/60
- (21) International Application Number: PCT/US01/11911
- (22) International Filing Date: 11 April 2001 (11.04.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
60/195,963 11 April 2000 (11.04.2000) US
09/809,367 15 March 2001 (15.03.2001) US
- (71) Applicant: **MASTERCARD INTERNATIONAL INCORPORATED** [US/US]: 2000 Purchase Street, Purchase, NY 10577-2509 (US).
- (72) Inventors: **HOGAN, Edward, J.**; 14 N. Chatworth Avenue, Larchmont, NY 10538 (US). **CAMPBELL, Carl, M.**; 809 Marlin Road, Newton Square, PA 19073 (US).
- (74) Agent: **SCHEINFELD, Robert, C.**; Baker Botts L.L.P., 30 Rockefeller Plaza, New York, NY 10112-0228 (US).
- (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW). Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM). European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR). OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).
- Published:
— with international search report
- (88) Date of publication of the international search report:
28 February 2002
- For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

(54) Title: AN IMPROVED METHOD AND SYSTEM FOR CONDUCTING SECURE PAYMENTS OVER A COMPUTER NETWORK



(57) Abstract: A method is provided for conducting a financial transaction by a purchaser with a merchant having an acquirer bank, over a communications network. The method includes the steps of sending a first authorization request using a pseudo account number associated with a real account number to a service provider which forwards a second authorization request to the issuer using the real account number and preferably a pseudo acquirer code associated with the service provider such that the response to the second request is based on the real account number and sent back to the service provider who preferably forwards a response to the first request preferably to the "real" acquirer. A message authentication code is further provided which includes transaction data, and where the authorization request is formatted as a standard payment card track having one or more fields including a discretionary field in which the message authentication code is placed.

INTERNATIONAL SEARCH REPORT

Inⁿ national Application No.

PCT/US 01/11911

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F19/00 G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G07F G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|------------|--|-----------------------|
| P, A | EP 1 028 401 A (CITIBANK NA) 16 August 2000 (2000-08-16) paragraph '0026! - paragraph '0027! paragraph '0044! - paragraph '0045! paragraph '0051! figure 2 --- | 1,5,9 |
| P, A | EP 1 017 030 A (IBM) 5 July 2000 (2000-07-05) paragraph '0056! claims 1,9-11 --- | 1,5,9 |
| A | US 5 883 810 A (ROSEN DANIEL ET AL) 16 March 1999 (1999-03-16) cited in the application column 2, line 17 - line 63 column 4, line 48 - column 5, line 22 --- -/-- | 1,5,9 |



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents:

A document defining the general state of the art which is not considered to be of particular relevance

E earlier document but published on or after the international filing date

L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

O document referring to an oral disclosure, use, exhibition or other means

P document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

Z document member of the same patent family

Date of the actual completion of the international search

27 November 2001

Date of mailing of the international search report

06/12/2001

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040. Tx. 31 651 epo nl.
Fax: (+31-70) 340-3016

Authorized officer

Wolles, B

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/US 01/11911

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|------------|---|-----------------------|
| A | US 5 678 010 A (PALMER LLOYD S ET AL) 14 October 1997 (1997-10-14) page 2, line 40 - line 61 ----- | 1,5,9 |

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 01/11911

| Patent document cited in search report | | Publication date | Patent family member(s) | Publication date |
|---|---|---------------------|---|--|
| EP 1028401 | A | 16-08-2000 | CN 1266240 A EP 1028401 A2 JP 2000322486 A | 13-09-2000 16-08-2000 24-11-2000 |
| EP 1017030 | A | 05-07-2000 | EP 1017030 A2 JP 2000194770 A | 05-07-2000 14-07-2000 |
| US 5883810 | A | 16-03-1999 | NONE | |
| US 5678010 | A | 14-10-1997 | AU 2692399 A AU 701815 B2 AU 6110396 A CA 2223178 A1 DE 19681450 C2 DE 19681450 T0 GB 2319108 A ,B WO 9642150 A2 | 24-06-1999 04-02-1999 09-01-1997 27-12-1996 10-08-2000 23-07-1998 13-05-1998 27-12-1996 |